IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

COREY HEARD, individually and on behalf of all others similarly situated,	)	
	)	**Case No. 1:19-cv-4158**
Plaintiff,	)	
	)	**Honorable Rebecca R. Pallmeyer**
v.	)	
	)	**Magistrate Judge Hon. Gabriel A. Fuentes**
BECTON, DICKINSON & COMPANY,	)	
	)	
Defendant.	)	

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff Corey Heard ("Plaintiff" or "Heard") individually and on behalf of all others similarly situated (the "Class"), by and through his attorneys, brings the following Class Action Complaint ("Complaint") pursuant to the Illinois Code of Civil Procedure, 735 ILCS §§ 5/2-801 and 2-802, against Becton, Dickinson & Company ("Becton" or "Defendant"), its subsidiaries and affiliates, to redress and curtail Defendant's unlawful collection, obtainment, use, storage, and disclosure of Plaintiff's sensitive and proprietary biometric data. Plaintiff alleges as follows upon personal knowledge as to himself, his own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by his attorneys.

NATURE OF THE ACTION

1. Defendant Becton is a leading manufacturer of medical technology that produces and sells medical devices, instrument systems, and reagents. Becton sells its products and services to healthcare institutions, science researchers, clinical laboratories, and the pharmaceutical industry, among others. Becton manufactures the Pyxis MedStation system, and related Pxyis devices (collectively referred to as "Pyxis"), all of which are automated medication dispensing

systems that require their users to scan a fingerprint to access the system. In Illinois alone, Becton provides Pyxis devices to dozens of hospitals, including St. Bernard Hospital, Norwegian American Hospital, Community First Medical Center, Weiss Memorial Hospital, Advocate Illinois Masonic Hospital, Northwestern Lake Forest Hospital, and Northwestern Memorial Hospital, amongst others.

2. To use its Pyxis devices, Becton requires users to scan their biometric information, namely their fingerprint. Within a single hospital location, there are typically multiple Pyxis devices. Once a user has enrolled and registered his or her fingerprint with the system, they have access to multiple Pyxis devices within that hospital.

3. Pyxis devices, like other biometric technology, authenticate user identities by capturing and utilizing their biometric identifiers and/or information. The Pyxis device software allows devices, systems and servers to communicate with one another.

4. There are two high-level phases Pyxis devices engage in to authenticate user identities. In the first phase, the user enrolls his or her fingerprint with the device. And in the second phase, depending on configuration, the device can verify or identify the user's fingerprint.

5. Specifically, when a Pyxis device is configured to verify a user, it compares the input fingerprints against every set of fingerprints enrolled on the device and stored in the system to confirm it matches a single, pre-selected, previously-enrolled set of the user's fingerprints. When a Pyxis device is configured to identify a user, it compares the input fingerprints against the universe of fingerprints enrolled in the device and stored in the system to find and match the user.

6. To enroll their biometric identifiers with the Pyxis device, the user places their finger on the Pyxis device's "platen," the flat, window-like plate located on the device's fingerprint scanner, where the device captures an image of their fingerprint. From the image, unique features

are extracted to create a unique template associated with the user, which is stored directly on the device, as well as in a database. Each time the user subsequently provides their fingerprint, the device compares the unique features of the input fingerprint against the stored template to verify or identify the user.

7. Pyxis devices are configured so that functional processing and storage of the unique user templates are shared with Becton's servers.

8. Becton markets its Pyxis devices to hospitals as one component of an integrated medication management platform, through which Becton provides a single, centralized location for hospitals to manage data, along with dedicated support services which Becton can access the biometric data collected. *Available at* https://www.bd.com/en-us/offerings/integrated-solutions/medication-management-solutions.

9. Thus, Becton specifically designs and constructs its Pyxis devices so that the fingerprint data it collects and obtains, from templates to data extracted from subsequent fingerprint scans, is managed, maintained, and stored on its servers.

10. Unlike ID badges or key fobs – which can be changed or replaced if stolen or compromised – fingerprints are unique, permanent biometric identifiers associated with each employee. This exposes employees who are required to use Pyxis devices as a condition of their employment to serious and irreversible privacy risks. For example, if a database containing fingerprints or other sensitive, proprietary biometric data is hacked, breached, or otherwise exposed – like in the recent Google+, Equifax, Uber, Facebook/Cambridge Analytica, and Marriott data breaches or misuses – employees have ***no*** means by which to prevent identity theft, unauthorized tracking or other unlawful or improper use of this highly personal and private information.

11. Biometrics are not relegated to esoteric corners of commerce. Many businesses – such as hospitals – and financial institutions have incorporated biometric applications into their workplace in the form of biometric timeclocks, and into consumer products, including such ubiquitous consumer products as checking accounts and cell phones.

12. In 2015, a data breach at the United States Office of Personnel Management exposed the personal identification information, including biometric data, of over 21.5 million federal employees, contractors, and job applicants. U.S. Off. of Personnel Mgmt., *Cybersecurity Incidents* (2018), *available at* www.opm.gov/cybersecurity/cybersecurity-incidents.

13. An illegal market already exists for biometric data. Hackers and identity thieves have targeted Aadhaar, the largest biometric database in the world, which contains the personal and biometric data – including fingerprints, iris scans, and a facial photograph – of over a billion Indian citizens. *See* Vidhi Doshi, *A Security Breach in India Has Left a Billion People at Risk of Identity Theft*, The Washington Post (Jan. 4, 2018), *available at* https://www.washingtonpost.com/news/worldviews/wp/2018/01/04/a-security-breach-in-india-has-left-a-billion-people-at-risk-of-identity-theft/?utm_term=.b3c70259f138.

14. In January 2018, an Indian newspaper reported that the information housed in Aadhaar was available for purchase for less than $8 and in as little as 10 minutes. Rachna Khaira, *Rs 500, 10 Minutes, and You Have Access to Billion Aadhaar Details*, The Tribune (Jan. 4, 2018), *available at* http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html.

15. Recognizing the need to protect its citizens from situations like these, Illinois enacted the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.*, specifically to

regulate companies that collect, obtain, store and use Illinois citizens' biometrics, such as fingerprints.

16. Notwithstanding the clear and unequivocal requirements of the law, Defendant disregards Pyxis users' statutorily protected privacy rights and unlawfully collects, obtains, stores, disseminates, and uses their biometric data in violation of BIPA. Specifically, Defendant has violated and continues to violate BIPA because it did not and continues not to:

a. Properly inform Plaintiff and others similarly situated in writing of the specific purpose and length of time for which their fingerprints were being collected, obtained, stored, and used, as required by BIPA;

b. Receive a written release from Plaintiff and others similarly situated to collect, obtain, store, or otherwise use their fingerprints, as required by BIPA;

c. Provide a publicly available retention schedule and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' fingerprints, as required by BIPA; and

d. Obtain consent from Plaintiff and others similarly situated to disclose, redisclose, or otherwise disseminate their fingerprints to a third party as required by BIPA.

17. Plaintiff and other similarly-situated individuals are aggrieved because they were not: (1) informed in writing of the purpose and length of time for which their fingerprints were being collected, obtained, stored, disseminated and used; (2) provided a publicly available retention schedule or guidelines for permanent destruction of the biometric data; and (3) provided (nor did they execute) a written release, as required by BIPA.

18. Defendant improperly discloses Pyxis user's fingerprint data to other, currently unknown, third parties, including, but not limited to third parties that host biometric data in their data center(s).

19. Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and other similarly-situated individuals' biometric data and have not and will not destroy their biometric data as required by BIPA.

20. Plaintiff and others similarly situated are aggrieved by Defendant's failure to destroy their biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the user's last interactions with Pyxis.

21. Plaintiff and others similarly situated have suffered an injury in fact based on Defendant's improper disclosures of their biometric data to third parties.

22. Plaintiff and others similarly situated have suffered an injury in fact based on Defendant's violations of their legal rights.

23. These violations have raised a material risk that Plaintiff's and other similarly-situated individuals' biometric data will be unlawfully accessed by third parties.

24. Pyxis users have a proprietary right to control their biometric information. In failing to comply with the requirements of BIPA, Defendant intentionally interferes with each user's right of possession and control over their valuable, unique, and permanent biometric data.

25. Defendant is directly liable for, and had actual knowledge of, the BIPA violations alleged herein.

26. Accordingly, Plaintiff seeks an Order: (1) declaring that Defendant's conduct violates BIPA; (2) requiring Defendant to cease the unlawful activities discussed herein; and (3) awarding statutory damages to Plaintiff and the proposed Class.

PARTIES

27. Plaintiff Corey Heard is a natural person and a resident of the State of Illinois.

28. Defendant Becton, Dickinson & Company is a New Jersey corporation that is registered to do business in Illinois.

JURISDICTION AND VENUE

29. This matter was removed from the Circuit Court of Cook County, Illinois. (*See* D.E. 1.)

30. The removing defendant, Becton, asserted that jurisdiction is proper under 28 U.S.C. §§ 1332(a), 1332(d), 1441, 1446, and 1453(b). (*See id.* at 3-4.).

FACTUAL BACKGROUND

I. The Biometric Information Privacy Act

31. In the early 2000s, major national corporations started using Chicago and other locations in Illinois to test "new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias." 740 ILCS § 14/5(c). Given its relative infancy, an overwhelming portion of the public became weary of this then-growing yet unregulated technology. *See* 740 ILCS § 14/5.

32. In late 2007, a biometrics company called Pay by Touch, which provided major retailers throughout the State of Illinois with fingerprint scanners to facilitate consumer transactions, filed for bankruptcy. That bankruptcy was alarming to the Illinois Legislature because suddenly there was a serious risk that millions of fingerprint records – which, like other unique biometric identifiers, can be linked to people's sensitive financial and personal data – could now be sold, distributed, or otherwise shared through the bankruptcy proceedings without adequate protections for Illinois citizens. The bankruptcy also highlighted the fact that most consumers who used the company's fingerprint scanners were completely unaware that the scanners were not actually transmitting fingerprint data to the retailer who deployed the scanner, but rather to the

now-bankrupt company, and that their unique biometric identifiers could now be sold to unknown third parties.

33. Recognizing the "very serious need [for] protections for the citizens of Illinois when it [came to their] biometric information," Illinois enacted BIPA in 2008. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276; 740 ILCS § 14/5.

34. Additionally, to ensure compliance, BIPA provides that, for each violation, the prevailing party may recover $1,000 or actual damages, whichever is greater, for negligent violations and $5,000, or actual damages, whichever is greater, for intentional or reckless violations. 740 ILCS 14/20.

35. BIPA is an informed consent statute which achieves its goal by making it unlawful for a company to, among other things, collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first:

a. Informs the subject in writing that a biometric identifier or biometric information is being collected, stored and used;

b. Informs the subject in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, obtained, stored, and used; and

c. Receives a written release executed by the subject of the biometric identifier or biometric information.

See 740 ILCS § 14/15(b).

36. Biometric identifiers include retina and iris scans, voiceprints, scans of hand and face geometry, and – most importantly here – fingerprints. *See* 740 ILCS § 14/10. Biometric information is separately defined to include any information based on an individual's biometric identifier that is used to identify an individual. *Id*.

37. BIPA also establishes standards for how companies must handle Illinois citizens' biometric identifiers and biometric information. *See, e.g.,* 740 ILCS § 14/15(c)-(d). For example, BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for such disclosure. *See* 740 ILCS § 14/15(d)(1).

38. BIPA also prohibits selling, leasing, trading, or otherwise profiting from a person's biometric identifiers or biometric information (740 ILCS § 14/15(c)) and requires companies to develop and comply with a written policy – made available to the public – establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting such identifiers or information has been satisfied or within three years of the individual's last interaction with the company, whichever occurs first. 740 ILCS § 14/15(a).

39. The Illinois legislature enacted BIPA due to the increasing use of biometric data in financial and security settings, the general public's hesitation to use biometric information, and – most significantly – the unknown ramifications of biometric technology. Biometrics are biologically unique to the individual and, once compromised, an individual is at heightened risk for identity theft and left without any recourse.

40. BIPA provides individuals with a private right of action, protecting their right to privacy regarding their biometrics as well as protecting their rights to know the precise nature for which their biometrics are used and how they are being stored and ultimately destroyed. Unlike other statutes that only create a right of action if there is a qualifying data breach, BIPA strictly regulates the manner in which entities may collect, obtain, store, use, and disseminate biometrics and creates a private right of action for lack of statutory compliance.

41. Plaintiff, like the Illinois legislature, recognizes how imperative it is to keep biometric information secure. Biometric information, unlike other personal identifiers such as a social security number, cannot be changed or replaced if hacked or stolen.

II. Defendant Violates the Biometric Information Privacy Act.

42. By the time BIPA passed through the Illinois legislature in mid-2008, most companies who had experimented using individuals' biometric data stopped doing so.

43. However, Defendant failed to take note of the shift in Illinois law governing the collection, use and dissemination of biometric data. As a result, Defendant continues to collect, obtain, store, use and disseminate Illinois employees' biometric data in violation of BIPA.

44. Specifically, new users are required to have their fingerprint scanned in on a Pyxis device in order to enroll them in the Pyxis database.

45. After users place their fingerprint on the platen portion of the Pyxis device to be scanned, the Pyxis device captures and/or obtains an image of the fingerprint. From that image, the device extracts unique features, like ridges or minutiae of a fingerprint. The device processes the extracted portions to create a unique template based on the fingerprint data.

46. The unique template created upon enrollment is stored and maintained on both the employer's and Becton's servers.

47. Once enrolled with a Pyxis device, users must provide their fingerprint every time they subsequently wish to access the device. The Pyxis device authenticates user identities by first extracting unique features from each subsequent input fingerprint provided, and then comparing the input fingerprint against the template fingerprint stored on the device. This process indicates whether the input fingerprint matches the enrolled fingerprint template stored on the device.

48. Becton designs and constructs Pyxis devices with a network interface, which provides transmission of fingerprint data collected and/or obtained from those devices to its servers and to third-parties who host that data.

49. Becton developed and markets an integrated medication management system, in which Becton actively manages, maintains, and stores data collected from Pyxis devices, including biometric data, in a single, centralized location on its servers.

50. Becton accesses its Pyxis servers for various purposes, including to facilitate support services for its clients.

51. Unfortunately, Becton fails to inform users of its Pyxis devices that it is collecting, obtaining, storing or using their sensitive biometric data, the extent of the purposes for which it collects and/or obtains their sensitive biometric data, or to whom the data is disclosed.

52. In those instances, Becton similarly fails to inform users of its Pyxis devices that Becton is collecting, obtaining, storing, or using their sensitive biometric data, the extent of the purposes for which it collects and/or obtains their sensitive biometric data, or to whom the data is disclosed.

53. Becton failed to establish and adhere to a written, publicly-available policy identifying its retention schedule and guidelines for permanently destroying users' biometric data when the initial purpose for collecting or obtaining their biometrics is no longer relevant, as required by BIPA.

54. In addition, Becton profits from the use of users' biometric data. For instance, Becton markets its Pyxis devices to employers as superior options to medication disbursement because they improve precision and accuracy of user access via biometric identification and allow for centralized management of data collected by the Pyxis devices. By marketing Pyxis in this

manner, Becton obtains a competitive advantage over automated medication companies and secures profits from its use of biometric data, all while failing to comply with the minimum requirements for handling users' biometric data established by BIPA.

55. The Pay by Touch bankruptcy that catalyzed the passage of BIPA highlights why such conduct – where individuals are aware that they are providing a fingerprint but not aware to whom or for what purposes they are doing so – is dangerous. That bankruptcy spurred Illinois citizens and legislators into realizing that it is crucial for individuals to understand when providing biometric identifiers, such as a fingerprint, who exactly is collecting or obtaining their biometric data, where it will be transmitted and for what purposes, and for how long. Defendant disregards these obligations and these employees' statutory rights and instead unlawfully collects, obtains, stores, uses and disseminates their biometric identifiers and information, without ever receiving the individual's informed written consent required by BIPA.

56. Remarkably, Defendant has created the same situation that Pay by Touch did by assembling a database of biometric data through broadly deployed fingerprint scanners, but failed to comply with the law specifically designed to protect individuals whose biometrics are collected in these circumstances. Defendant disregards these obligations and Illinois users' statutory rights and instead unlawfully collects, obtains, stores, uses, and disseminates users' biometric identifiers and information without ever receiving the individual's informed written consent required by BIPA.

57. Users are not told what might happen to their biometric data if and when Defendant merges with another company or worse, if and when Defendant's businesses folds, or when the other third parties that have received their biometric data businesses fold.

58. Since Defendant neither publishes a BIPA-mandated data-retention policy nor discloses the purposes for their collection, obtainment and use of biometric data, users have no idea whether Defendant sells, discloses, re-discloses, or otherwise disseminates their biometric data. Moreover, Plaintiff and others similarly situated are not told to whom Defendant currently discloses their biometric data to, or what might happen to their biometric data in the event of a merger or a bankruptcy.

59. These violations have raised a material risk that Plaintiff's and other similarly-situated individuals' biometric data will be unlawfully accessed by third parties.

60. By and through the actions detailed above, Defendant disregards Plaintiff's and other similarly-situated individuals' legal rights in violation of BIPA.

III. Plaintiff Heard's Experience

61. Plaintiff Corey Heard has worked as a respiratory therapist for multiple hospitals that utilize Pyxis, including St. Bernard Hospital from May 2015 until November 2017, Norwegian American Hospital in 2018, Community First Medical Center in 2018 and 2019, Weiss Memorial Hospital January in 2019 and Advocate Illinois Masonic Hospital March 2019 to the present ("the Hospitals").

62. Plaintiff was required to scan and enroll his fingerprint so it could be used as an authentication method to access the Pyxis devices.

63. Upon each occasion that Plaintiff began new employment with each of the Hospitals, Plaintiff was required to place his fingerprint on the platen of a Pyxis device in order to enroll his fingerprint on the devices and in each system.

64. Upon each occasion when Plaintiff placed his fingerprint on the platen of a Pyxis device, Defendant captured and/or obtained an image of his fingerprint, from which Defendant extracted unique features of his fingerprint to create a fingerprint template.

65. Defendant subsequently stored Plaintiff's unique fingerprint data, in the form of a unique, user-specific template, in its systems.

66. The Hospitals subsequently stored Plaintiff's fingerprint data, in the form of a unique, user-specific template, in their systems.

67. Plaintiff was required to scan his fingerprint each time he accessed the Pyxis devices.

68. Each time Plaintiff accessed a Pyxis device, Defendant collected and obtained Plaintiff's fingerprint data and stored it on its servers.

69. Plaintiff has never been informed of the specific limited purposes or length of time for which Defendant collected, obtained, stored, used and/or disseminated his biometric data.

70. Plaintiff has never been informed of any biometric data retention policy developed by Defendant, nor has he ever been informed of whether Defendant will ever permanently delete his biometric data.

71. Plaintiff has never been provided with nor ever signed a written release allowing Defendant to collect, obtain, store, use or disseminate his biometric data.

72. Plaintiff has continuously and repeatedly been exposed to the risks and harmful conditions created by Defendant's violations of BIPA as alleged herein.

73. No amount of time or money can compensate Plaintiff if his biometric data is compromised by the lax procedures through which Defendant captured, obtained, stored, used, and disseminated his and other similarly-situated individuals' biometrics. Moreover, Plaintiff

would not have provided his biometric data to Defendant if he had known that they would retain such information for an indefinite period of time without his consent.

74. A showing of actual damages is not necessary in order to state a claim under BIPA. *See Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 40 ("[A]n individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an "aggrieved" person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act"). Nonetheless, Plaintiff has been aggrieved because he suffered an injury-in-fact based on Defendant's violations of his legal rights. Defendant intentionally interfered with Plaintiff's right to possess and control his own sensitive biometric data. Additionally, Plaintiff suffered an invasion of a legally protected interest when Defendant secured his personal and private biometric data at a time when they had no right to do so, a gross invasion of his right to privacy. BIPA protects users like Heard from this precise conduct. Defendant had no lawful right to secure this data or share it with third parties absent a specific legislative license to do so.

75. Plaintiff's biometric information is economically valuable, and such value will increase as the commercialization of biometrics continues to grow. As such, Plaintiff was not sufficiently compensated by Defendant for its retention and use of his and other similarly-situated employees' biometric data. Plaintiff would not have agreed to enroll fingerprint data in Defendant's systems if he had known that Defendant would retain his biometric data indefinitely.

76. Plaintiff also suffered an informational injury because Defendant failed to provide him with information to which he was entitled by statute. Through BIPA, the Illinois legislature has created a right: an employee's right to receive certain information prior to an employer securing their highly personal, private and proprietary biometric data; and an injury – not receiving this extremely critical information.

77. Plaintiff also suffered an injury in fact because Defendant improperly disseminated his biometric identifiers and/or biometric information to third parties that hosted the biometric data in their data centers, in violation of BIPA.

78. Pursuant to 740 ILCS 14/15(b), Plaintiff was entitled to receive certain information prior to Defendant securing his biometric data; namely, information advising him of the specific limited purpose(s) and length of time for which Defendant collects, obtains, stores, uses and disseminates his private biometric data; information regarding Defendant's biometric retention policy; and, a written release allowing Defendant to collect, obtain, store, use, and disseminate his private biometric data. By depriving Plaintiff of this information, Defendant injured him. *Public Citizen v. U.S. Department of Justice*, 491 U.S. 440, 449 (1989); *Federal Election Commission v. Akins*, 524 U.S. 11 (1998).

79. Plaintiff has plausibly inferred actual and ongoing harm in the form of monetary damages for the value of the collection and retention of his biometric data; in the form of monetary damages by not obtaining additional compensation as a result of being denied access to material information about Defendant's policies and practices; in the form of the unauthorized disclosure of his confidential biometric data to third parties; in the form of interference with his right to control and possess his confidential biometric data; and, in the form of the continuous and ongoing exposure to substantial and irreversible loss of privacy.

80. As Plaintiff is not required to allege or prove actual damages in order to state a claim under BIPA, he seeks statutory damages under BIPA as compensation for the injuries caused by Defendant. *Rosenbach*, 2019 IL 123186, ¶ 40.

CLASS ALLEGATIONS

81. Pursuant to the Illinois Code of Civil Procedure, 735 ILCS 5/2-801, Plaintiff brings

claims on his own behalf and as a representative of all other similarly-situated individuals pursuant to BIPA, 740 ILCS § 14/1, *et seq.*, to recover statutory penalties, prejudgment interest, attorneys' fees and costs, and other damages owed.

82. As discussed *supra*, Section 14/15(b) of BIPA prohibits a company from, among other things, collecting, capturing, purchasing, receiving through trade, or otherwise obtaining a person's or a customer's biometric identifiers or biometric information, unless it first (1) informs the individual in writing that a biometric identifier or biometric information is being collected, obtained or stored; (2) informs the individual in writing of the specific purpose and length of time for which a biometric identifier or biometric information is being collected, obtained, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information. 740 ILCS § 14/15.

83. Plaintiff seeks class certification under the Illinois Code of Civil Procedure, 735 § ILCS 5/2-801 for the following class of similarly-situated individuals under BIPA:

> All users in the State of Illinois who had their fingerprints collected, captured, received, or otherwise obtained or disclosed by Defendant during the applicable statutory period.

84. This action is properly maintained as a class action under 735 ILCS § 5/2-801 because:

A. The class is so numerous that joinder of all members is impracticable;

B. There are questions of law or fact that are common to the class;

C. The claims of the Plaintiff are typical of the claims of the class; and,

D. The Plaintiff will fairly and adequately protect the interests of the class.

Numerosity

85. The total number of putative class members exceeds fifty (50) individuals. The exact number of class members can easily be determined from Becton's records.

Commonality

86. There is a well-defined commonality of interest in the substantial questions of law and fact concerning and affecting the Class in that Plaintiff and all members of the Class have been harmed by Defendant's failure to comply with BIPA. The common questions of law and fact include, but are not limited to the following:

A. Whether Defendant collected, captured or otherwise obtained Plaintiff's and the Class's biometric identifiers or biometric information;

B. Whether Defendant properly informed Plaintiff and the Class of its purposes for collecting, obtaining, using, storing and disseminating their biometric identifiers or biometric information;

C. Whether Defendant obtained a written release (as defined in 740 ILCS § 14/10) to collect, obtain, use, store and disseminate Plaintiff's and the Class's biometric identifiers or biometric information;

D. Whether Defendant has disclosed or re-disclosed Plaintiff's and the Class's biometric identifiers or biometric information;

E. Whether Defendant has sold, leased, traded, or otherwise profited from Plaintiff's and the Class's biometric identifiers or biometric information;

F. Whether Defendant developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within three years of its last interaction with the individual, whichever occurs first;

G. Whether Defendant complies with any such written policy (if one exists);

H. Whether Defendant used Plaintiff's and the Class's fingerprints to identify them;

I. Whether Defendant's violations of BIPA have raised a material risk that Plaintiff's biometric data will be unlawfully accessed by third parties;

J. Whether the violations of BIPA were committed negligently; and

K. Whether the violations of BIPA were committed intentionally and/or recklessly.

87. Plaintiff anticipates that Defendant will raise defenses that are common to the class.

Adequacy

88. Plaintiff will fairly and adequately protect the interests of all members of the class, and there are no known conflicts of interest between Plaintiff and class members. Plaintiff, moreover, has retained experienced counsel that are competent in the prosecution of complex litigation and who have extensive experience acting as class counsel.

Typicality

89. The claims asserted by Plaintiff are typical of the class members he seeks to represent. Plaintiff has the same interests and suffers from the same unlawful practices as the class members.

90. Upon information and belief, there are no other class members who have an interest individually controlling the prosecution of his or her individual claims, especially in light of the relatively small value of each claim and the difficulties involved in bringing individual litigation against one's employer. However, if any such class member should become known, he or she can "opt out" of this action pursuant to 735 ILCS § 5/2-801.

Predominance and Superiority

91. The common questions identified above predominate over any individual issues, which will relate solely to the quantum of relief due to individual class members. A class action is superior to other available means for the fair and efficient adjudication of this controversy because individual joinder of the parties is impracticable. Class action treatment will allow a large number of similarly-situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of effort and expense if these claims were brought individually. Moreover, as the damages suffered by each class member are relatively small in the sense pertinent to class action analysis, the expenses and burden of individual litigation

would make it difficult for individual class members to vindicate their claims.

92. Additionally, important public interests will be served by addressing the matter as a class action. The cost to the court system and the public for the adjudication of individual litigation and claims would be substantially more than if claims are treated as a class action. Prosecution of separate actions by individual class members would create a risk of inconsistent and varying adjudications, establish incompatible standards of conduct for Defendant and/or substantially impair or impede the ability of class members to protect their interests. The issues in this action can be decided by means of common, class-wide proof. In addition, if appropriate, the Court can and is empowered to fashion methods to efficiently manage this action as a class action.

FIRST CAUSE OF ACTION
Violation of 740 ILCS § 14/15(a): Failure to Institute, Maintain and Adhere to Publicly-Available Retention Schedule

93. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

94. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention – and, importantly, deletion – policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric information. *See* 740 ILCS § 14/15(a).

95. Defendant fails to comply with these BIPA mandates.

96. Defendant Becton is a corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

97. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected and/or obtained by Defendant (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

98. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

99. Defendant failed to provide a publicly available retention schedule or guidelines for permanently destroying biometric identifiers and biometric information as specified by BIPA. *See* 740 ILCS § 14/15(a).

100. Defendant lacks retention schedules and guidelines for permanently destroying Plaintiff's and the Class's biometric data and has not and will not destroy Plaintiff's and the Class's biometric data when the initial purpose for collecting or obtaining such data has been satisfied or within three years of the individual's last interaction with the company.

101. On behalf of himself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, obtainment, storage, and use of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

SECOND CAUSE OF ACTION
Violation of 740 ILCS § 14/15(b): Failure to Obtain Informed Written Consent and Release Before Obtaining Biometric Identifiers or Information

102. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

103. BIPA requires companies to obtain informed written consent from employees before acquiring their biometric data. Specifically, BIPA makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information unless [the entity] first: (1) informs the subject…in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject…in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; ***and*** (3) receives a written release executed by the subject of the biometric identifier or biometric information…" 740 ILCS 14/15(b) (emphasis added).

104. Defendant fails to comply with these BIPA mandates.

105. Defendant Becton is a corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

106. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected and/or obtained by Defendant (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

107. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

108. Defendant systematically and automatically collected, obtained, used, stored and disseminated Plaintiff's and the Class's biometric identifiers and/or biometric information without first obtaining the written release required by 740 ILCS 14/15(b)(3).

109. Defendant did not inform Plaintiff and the Class in writing that their biometric identifiers and/or biometric information were being collected, obtained, stored, used and disseminated, nor did Defendant inform Plaintiff and the Class in writing of the specific purpose(s)

and length of term for which their biometric identifiers and/or biometric information were being collected, obtained, stored, used and disseminated as required by 740 ILCS 14/15(b)(1)-(2).

110. By collecting, obtaining, storing, using and disseminating Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Defendant violated Plaintiff's and the Class's rights to privacy in their biometric identifiers and/or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq*.

111. On behalf of himself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, obtainment, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

THIRD CAUSE OF ACTION
Violation of 740 ILCS § 14/15(d): Disclosure of Biometric Identifiers and Information Before Obtaining Consent

112. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

113. BIPA prohibits private entities from disclosing a person's or customer's biometric identifier or biometric information without first obtaining consent for that disclosure. *See* 740 ILCS 14/15(d)(1).

114. Defendant fails to comply with this BIPA mandate.

115. Defendant Becton is a corporation registered to do business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS § 14/10.

116. Plaintiff and the Class are individuals who have had their "biometric identifiers" collected and/or obtained by Defendant (in the form of their fingerprints), as explained in detail in Sections II and III, *supra*. *See* 740 ILCS § 14/10.

117. Plaintiff's and the Class's biometric identifiers were used to identify them and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS § 14/10.

118. Defendant systematically and automatically disclosed, redisclosed, or otherwise disseminated Plaintiff's and the Class's biometric identifiers and/or biometric information without first obtaining the consent required by 740 ILCS 14/15(d)(1).

119. By disclosing, redisclosing, or otherwise disseminating Plaintiff's and the Class's biometric identifiers and biometric information as described herein, Defendant violated Plaintiff's and the Class's rights to privacy in their biometric identifiers and/or biometric information as set forth in BIPA. *See* 740 ILCS 14/1, *et seq.*

120. On behalf of himself and the Class, Plaintiff seeks: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiff and the Class by requiring Defendant to comply with BIPA's requirements for the collection, obtainment, storage, use and dissemination of biometric identifiers and biometric information as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS § 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3).

PRAYER FOR RELIEF

Wherefore, Plaintiff Corey Heard respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff Corey Heard as Class Representative, and appointing Stephan Zouras, LLP, as Class Counsel;

B. Declaring that Defendant's actions, as set forth above, violate BIPA;

C. Awarding statutory damages of $5,000 for *each* intentional and/or reckless violation of BIPA pursuant to 740 ILCS § 14/20(2) or, in the alternative, statutory damages of $1,000 for *each* negligent violation of BIPA pursuant to 740 ILCS § 14/20(1);

D. Declaring that Defendant's actions, as set forth above, were intentional or reckless;

E. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including an Order requiring Defendant to collect, obtain, store, use, destroy and disseminate biometric identifiers and/or biometric information in compliance with BIPA;

F. Awarding Plaintiff and the Class their reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS § 14/20(3);

G. Awarding Plaintiff and the Class pre- and post-judgment interest, to the extent allowable; and,

H. Awarding such other and further relief as equity and justice may require.

Date: March 31, 2020

Respectfully Submitted,

/s/ James B. Zouras

Ryan F. Stephan
James B. Zouras
Catherine T. Mitchell
Haley R. Jenkins
STEPHAN ZOURAS, LLP
100 N. Riverside Plaza
Suite 2150
Chicago, Illinois 60606
312.233.1550
312.233.1560 *f*
jzouras@stephanzouras.com
rstephan@stephanzouras.com
cmitchell@stephanzouras.com
hjenkins@stephanzouras.com
Firm ID: 43734

ATTORNEYS FOR PLAINTIFF

CERTIFICATE OF SERVICE

I, the attorney, hereby certify that on March 31, 2020, I filed the attached with the Clerk of the Court using the ECF system, which will send such filing to all attorneys of record.

/s/ James B. Zouras